- 本資料は下記書籍を基に作成されたものです．文書の内容の正確さは保障出来ないため，正確な知識を求める方は原文を参照して下さい．

- 題目：コンピュータ・ウィルスが伝染るのはなんでだろう！？
- 著者：武井純考
- 発行年月日：2003年5月20日
- 出版社：小学館

ウィルスの歴史

名城大学理工学部
渡邊研究室
060428262 宮崎雄介

大まかな流れ

- ウィルスの起源
- 世界最初のマイコンウィルス
- ウィルスの進化
- 日本の事情
- 様々なウィルスの登場
- 新たなウィルスの幕開け
- まとめ

学術的なウィルスの起源

- Fred Cohen
  - 南カリフォルニア大学の学生
  - 自己増殖型プログラムを研究
  - 1984年米国セキュリティー学会で発表
- 事件発生
  - 彼の作ったプログラム（ウィルス）が拡散
  - 制御不可能

一般人への広がり

- 1971年初のマイクロコンピュータ登場
- 一般向けが多数登場⇒より広範囲に
- 80年代半ば、世界中にマイコンが普及
- 1986年初めての本格的なウィルスがパキスタンで登場

世界最初のマイコンウィルス

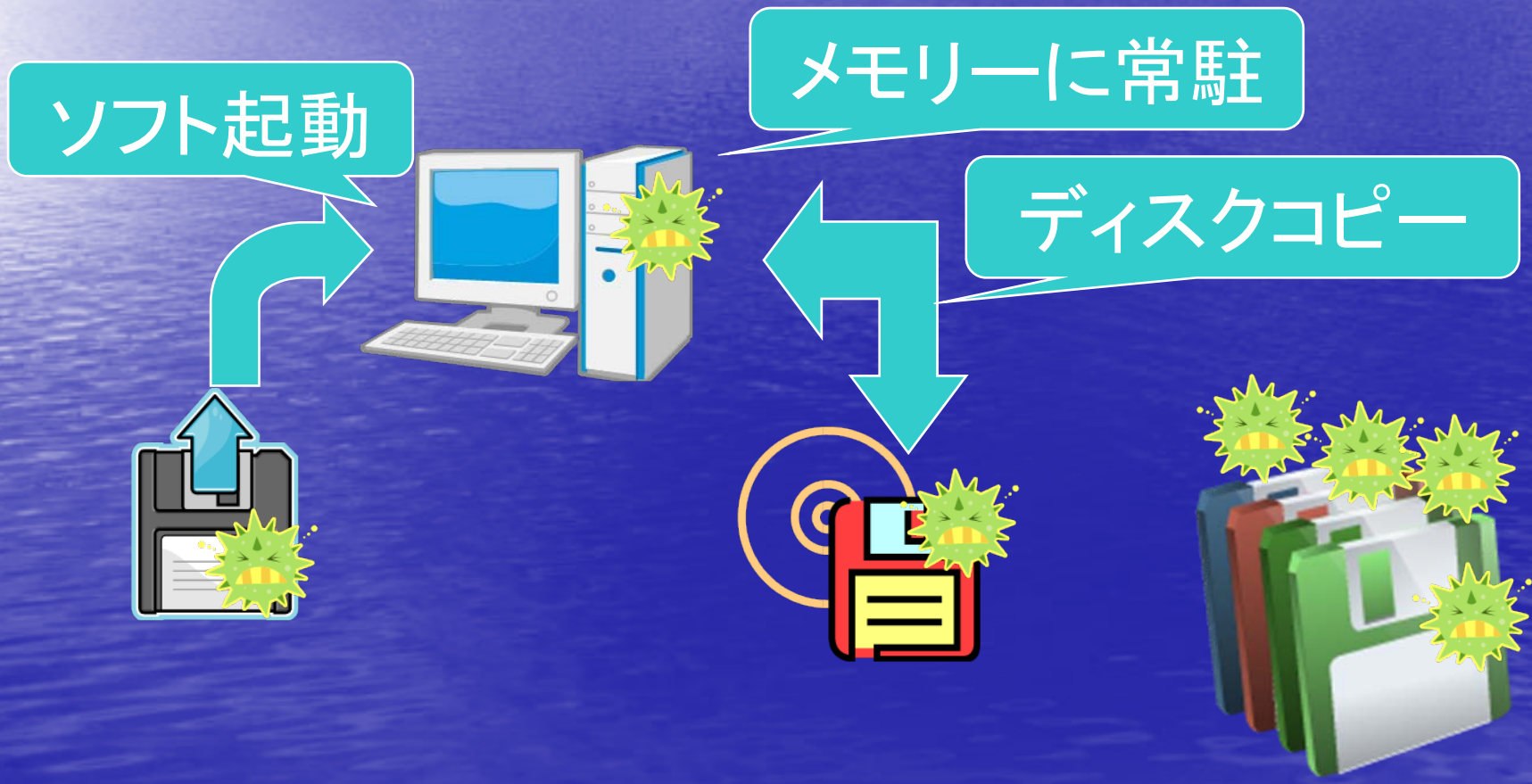
「ブレイン」ウィルス

- 作成者：ブレイン兄弟
- 職業：プログラマー
- 目的：自社製ソフトが不正コピーされたことを知る
- ディスクのコピー回数を検出する
- コピー回数が1以上の場合は不正コピー品

  ⇒自分たちに連絡を入れてもらうようなメッセージを表示

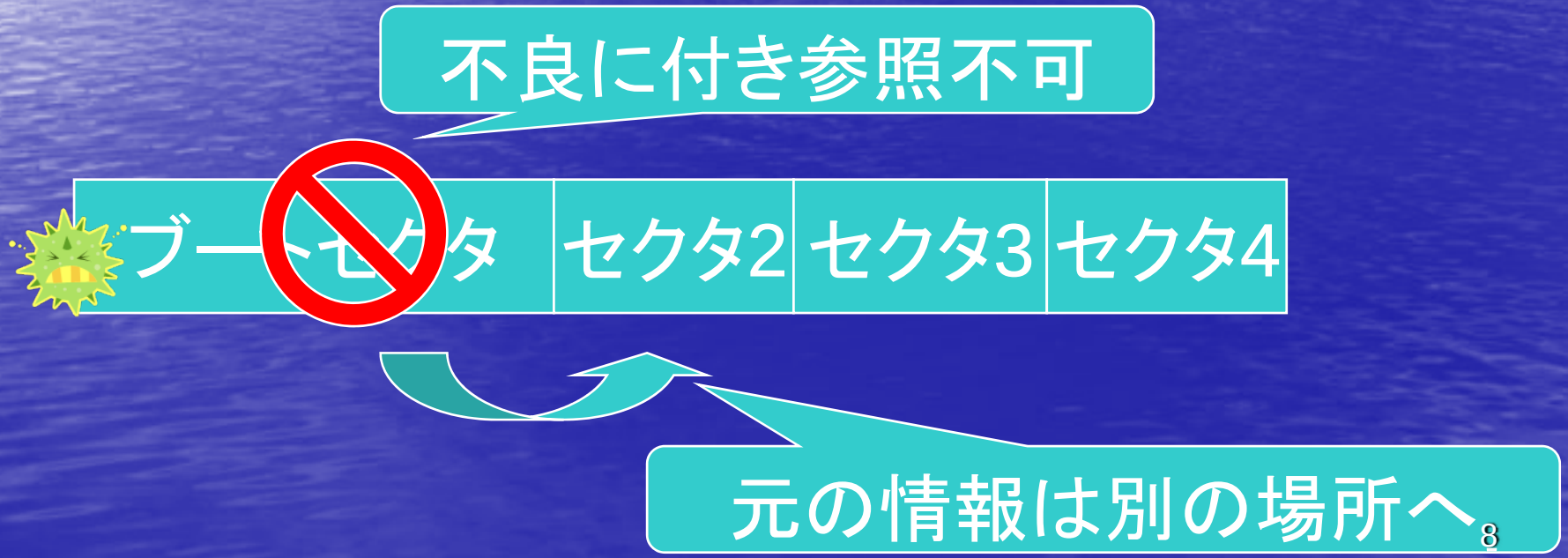
感染の仕組み

フロッピーディスクに潜むように作られている



ブートセクタとは

- ブートセクタには大切な情報が書かれている
- ディスクの起動に初めに読み込まれる場所
- ブートセクタを参照するような命令がきた場合は他の場所を参照させる



問題点

- 「彼らのソフトを起動したディスクとはまったく無関係なディスクがコピーされる可能性」を見落としていた

無関係なディスクへの流出

違法コピーしていなくてもメッセージが表示される

ウィルスの進化

「リーハイウィルス」（1987年11月）

- アメリカのリーハイ大学で発見
- ディスクのコピーのたびに新しいディスクに感染し、コピーされた回数を記録
- 回数が4回になると、ディスクの内容をすべて消去
- 動作や感染経路などの類似性から高確率でブレインウィルスが進化したウィルスと考えられる

進化とは？

- すべて**人間の仕業**
- ブレインウィルスを抽出して解析し、そこに改造を加えて新しい動作をするウィルスを作り上げた

改造

元のウィルス　　進化したウィルス

世界初のマイコン用ワクチン

- 1987年ブレインウィルスがアメリカに上陸し、報告が多数発生したときに登場
- ワームなどの駆除ソフトは以前から存在した
- マイコン用のウィルス駆除ソフトは初

  ⇒ブレインウィルスを除去するために開発された

日本の事情

- 当時の日本ではほとんど起こっていなかった
  - ブレインウィルスなども報告例なし

＜理由＞

- 独自規格のマシンを使用（海外はIBM PCなど）
- 1970年代の終わりに「NEC　PC-8001」発売
- その後も、「 PC-9801 」や後継機、シャープのXやMZシリーズ、富士通のFMシリーズ、MSXなど多数が乱立

国産ウィルスの登場

「SUR-GEONウィルス」（1989年）

- 新潟大学医学部生が中心のサークルが作成
- シャープのX68000専用
- フロッピーに感染
- 症状：毎年11月あるいは12月に感染したディスクが起動されると「SURGEON買ってね！ウヒョ」とメッセージが出力される。ハードディスクが接続されている場合はそのディスクを論理的に破壊する

国産アンチウィルスソフトの登場

- 1990年「サイバーワクチンいてこまし」が発売
- 日本コンピュータクラブ連盟が作成
- 大ヒット
- 駆除対象であるウィルスそのものはあまり広がっていなっかた

日本は平和だった

Java組み込みウィルスの登場

「StrangeBrew」（1998年8月）

- ワクチンメーカー（シマンテック）が発見
- Javaのソフトウェアに潜り込む
  - classファイルに寄生
  - Javaの動作する環境全てが感染対象
  - スタンドアローンで動作するJavaアプリケーションを実行
  - Javaアプレットは感染経路にはならない
  - 感染を行う以外の行動はしない

被害

- ファイルサイズが3,980バイト増加
- 101で割り切れる値になる
- タイムスタンプが変更される
- 他のclassファイルへの感染
- 元ファイルの実行にはほとんどの場合異常なし

Javaでもウィルスが作成可能

新たなウィルスの幕開け

「Melissa」（1999年3月下旬）

- 作成者：David
- メールを利用したウィルス
- タイトル「important message from 誰々」というメールが世界中のWindowsユーザーに届く。
  ※誰々・・・知人の名前
- 本文「こないだ頼まれたものだよ・・・誰にも見せるなよ(^__-)-☆」
- Word形式の添付ファイルあり

動作（被害）

- 添付ファイルを開くと、ドキュメントに仕込まれたスクリプトが起動
- メールソフトの送信履歴をもとに、感染者を送信者としてランダムに選んだ50人に送信
  - 電子式不幸の手紙（コンピュータ同士で送り合う）
- メールが大量に飛び交うことになる（50^n：nはメールが届く回数）

インターネットが麻痺状態

今までのウィルスと異なる点

- ウィルス？ワーム？人間に感染する病原体？
  - 区別が出来なくなった

＜定義＞

- ウィルス・・・何らかのファイルに感染
  ⇒メールに「添付」はされているが感染はしていない
- ワーム・・・プロセスが勝手に増殖して拡がっていく
  ⇒人間が実行しない限り何も起こらない
- 人間に感染する病原体
  ⇒人間の精神に働き掛け、手伝わせている

Melissaの登場後

「人間の精神に感染」を目指す傾向へ

通称「LoveLetter」「 LOVE YOU」ウィルス

- 作成者：23歳のフィリピン人学生
- 件名「I LOVE YOU」
- 本文「どうか添付の「私からきたLOVELETTER 」を見てください」
- 添付ファイル：LOVE-LETTER-FOR-YOU.TXT.vbs
  - ウィルス本体

動作（被害）

- mIRC（Internet Relay Chat）を利用し感染
- Internet Exprolerのホームページ設定を変更
- ウィルス本体をダウロード
- 感染したコンピュータに保存されているパスワードがあれば暗号化し、メールでフィリピンの特定のアドレスに送信しようとする
- コンピュータのレジストリを書き換える
  - コンピュータの起動ごとにウィルスを起動

被害

- ハードディスクにあるvbe, js, jse, css, wsh, sct, hta, jpg, jpeg, mp3, mp2をランダムに自分自身で上書きする

- ポイント
  - 人間に宛てたラブレターのように見える
  - コンピュータが人をだます

まとめ

- 「ウィルス」という言葉が学術的に用いられるようになったのは25年前
- 世界初のマイコンウィルスは故意ではなかった
- ウィルスの進化はすべて人の仕業である
- 現在のウィルスは人の精神を利用するようになった